US
924

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月１５日

出願番号
Application Number: 特願２００２－３３２４０４

[ST. 10/C]: ［ＪＰ２００２－３３２４０４］

出願人
Applicant(s): 日本電気株式会社
日本電気通信システム株式会社

２００３年　９月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７８９４９

【書類名】　特許願
【整理番号】　49200231
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/08
H04L 12/56
G06F 13/00
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　鈴木　一哉
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　地引　昌弘
【発明者】
【住所又は居所】　東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内
【氏名】　馬越　英之
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【特許出願人】
【識別番号】　000232254
【氏名又は名称】　日本電気通信システム株式会社
【代理人】
【識別番号】　100088890
【弁理士】
【氏名又は名称】　河原　純一
【手数料の表示】
【予納台帳番号】　009690
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9001717

【包括委任状番号】　9002497

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　マルチキャスト配信システムにおける鍵交換方式

【特許請求の範囲】

【請求項１】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、

復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項２】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャス

トパケット中の暗号化データの復号化を行うクライアントと、
暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと
を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。
【請求項３】　コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での復号鍵の問合せ・要求先の設定を不要にすることを特徴とする請求項１または請求項２記載のマルチキャスト配信システムにおける鍵交換方式。
【請求項４】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、
使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、
使用中の鍵の残り有効時間が第１設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、
マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、
使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、
コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、

その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、
使用中の鍵の残り有効時間が第２設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、
使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、
コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段と
を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。
【請求項５】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、
使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、
使用中の鍵の残り有効時間が第１設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替え

るコンテンツサーバ内の鍵管理手段と、
マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、
使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、
コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、
使用中の鍵の残り有効時間が第２設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、
使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、
コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段と

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項６】　コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先の設定を不要にすることを特徴とする請求項４または請求項５記載のマルチキャスト配信システムにおける鍵交換方式。

【請求項７】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

コンテンツサーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持する鍵情報管理テーブル，使用中の鍵の残り有効時間が第１設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存する鍵管理手段，ならびにマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、

クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル，コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段，および使用中の鍵の残り有効時間が第２設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵

管理手段として機能させるためのクライアント用鍵交換制御プログラムと、
鍵管理サーバを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル，およびコンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと
を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。
【請求項８】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、
コンテンツサーバを、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル，使用中の鍵の残り有効時間が第１設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段，およびマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、
クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル，コンテンツサーバから送信されてきたマルチキャストパケッ

トを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段，および使用中の鍵の残り有効時間が第２設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるためのクライアント用鍵交換制御プログラムと、

鍵管理サーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル，およびコンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐマルチキャスト配信システムに関し、鍵（暗号鍵／復号鍵）の交換を制御・管理するためのマルチキャスト配信システムにおける鍵交換方式に関する。

【０００２】

【従来の技術】

一般に、マルチキャストのパケットは不特定多数の受信者によって受信されるので、特定のクライアントのみに視聴を許可するためには、当該パケットによって配信されるデータに対して暗号鍵による暗号化を施し、視聴を許可したクライアントにのみ復号鍵を配布する必要がある。

【０００３】

このとき、定期的に鍵を変更することで、クライアントを管理し、さらに暗号の秘匿性を向上させることができる。

【０００４】

従来より、配信データ（配信対象のデータ）の暗号化が行われるマルチキャスト配信システムにおいては、一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐために、暗号鍵や復号鍵の交換が行われていた（例えば、特許文献１参照）。

【０００５】

このような従来のマルチキャスト配信システムは、コンテンツサーバ（特許文献１では「送信部」と表現されている）とクライアント（特許文献１では「受信部」と表現されている）と鍵管理サーバとを含んで構成されており、コンテンツサーバが一定時間毎に鍵要求情報を添付したパケットを送信し、それを受けたクライアントが鍵管理サーバに対して鍵を要求することで、一定時間毎に鍵を更新し、鍵が第三者に渡った際にも暗号化データが流出することを防いでいる。

【０００６】

【特許文献１】

特開２００１－２８５２７３号公報（第２－４頁、図１）

【０００７】

【発明が解決しようとする課題】

上述した従来のマルチキャスト配信システムにおける鍵交換方式には、次のような問題点があった。

【０００８】

第１の問題点は、鍵要求情報の受信時にタイムラグが生じるという点である。このような問題点が存在する理由は、クライアントが鍵要求情報を受け取った際に、鍵管理サーバに対して鍵を要求しその要求の応答（鍵）を受けてから復号化を開始するため、鍵管理サーバから応答が帰ってくるまでクライアントは暗号化情報（暗号化データ）の復号化ができないからである。

【０００９】

第２の問題点は、放送途中にマルチキャスト放送に参加した場合は即時に視聴することができないという点である。このような問題点が存在する理由は、鍵要求情報が添付されたパケットは一定間隔毎に発生するものであるため、マルチキャスト放送に参加したクライアントは次の鍵要求情報が送られてくるまで復号鍵を取得できず、復号化ができないからである。

【００１０】

第３の問題点は、マルチキャスト配信した鍵要求情報が経路上で消失した際に鍵の取得ができない期間が長期になるおそれがあるという点である。このような問題点が存在する理由は、マルチキャスト配信は応答確認が行われないため、経路上でパケットが消失したことが確認できないので、鍵要求情報を添付したパケットが消失した場合に、次の鍵要求情報が送られてくるまで新しい鍵の取得ができないからである。したがって、新しい鍵が取得できるまで、暗号化情報の復号化ができないようになる。

【００１１】

本発明の目的は、上述の点に鑑み、以上の問題点を解決し、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐネットワークシステムにおいて、鍵の変更（交換）時の確認遅延（鍵交換遅延）をなくしてリアルタイムのデータの処理を可能にするマルチキャスト配信システムにおける鍵交換方式を提供することにある。

【００１２】

すなわち、本発明の特徴は、マルチキャスト配信時に配信データを暗号化する場合に、暗号鍵・復号鍵を定期的に変更することによって暗号の秘匿性を向上し、かつ、鍵変更時の新しい鍵情報（鍵およびそれに付随する情報）の取得（クライ

アントによる取得）に伴う遅延を防ぐことを可能にする点にある。

【００１３】

【課題を解決するための手段】

本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵・復号鍵（対となる暗号鍵および復号鍵。同じ鍵である場合もある）とその鍵番号（その鍵を識別するための情報）とその残り有効時間との組（その鍵に関する鍵情報）および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵（暗号鍵・復号鍵）の残り有効時間が第１設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり０よりも大きい値）となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージ（次に使用する復号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）を送信し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報（当該暗号鍵・復号鍵とその鍵番号とその残り有効時間との組）を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第２設定値（第１設定値よりも小さい値であり０より

も大きい値）となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有する。

【００１４】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル，鍵管理手段，および暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル，パケット受信・復号化手段，および鍵管理手段として機能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

【００１５】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および

残り有効時間とを管理し、使用中の鍵の有効時間内（残り有効時間が０となる前）に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

【００１６】

また、本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵の残り有効時間が第１設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり０よりも大きい値）となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えるコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号

鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第２設定値（第１設定値よりも小さい値であり０よりも大きい値）となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージ（当該次に使用する暗号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）をコンテンツサーバに返送し、使用中の鍵の残り有効時間が第２設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が０となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有するように構成することも可能である。

【００１７】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル，鍵管理手段，および暗号化・パ

ケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル，パケット受信・復号化手段，および鍵管理手段として機能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

【００１８】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

【００１９】

さらに、以上列挙した本発明のマルチキャスト配信システムにおける鍵交換方式においては、コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先（復号鍵の問合せ・要求先）の設定を不要にすることも可能である。

【００２０】

【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

【００２１】

（１）　第１の実施の形態

【００２２】

図１は、本発明の第１の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【００２３】

図１を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ１１と、コンテンツサーバ１１より送られたマルチキャストパケットを受信するクライアント５１，５２，…，５ｎ（ｎは正整数）と、コンテンツサーバ１１から送られた鍵情報メッセージ７１中の復号鍵に関する鍵情報を保管しクライアント５ｉ（ｉは１～ｎの正整数）からの鍵情報要求８１に対して応答メッセージ８２を送信する鍵管理サーバ３１と、コンテンツサーバ１１，クライアント５ｉ，および鍵管理サーバ３１を接続するネットワーク１００とを含んで構成されている。

【００２４】

コンテンツサーバ１１は、マルチキャストパケットによって配信されるデータ（配信データ）の暗号化・復号化に用いる鍵（暗号鍵・復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル２１を有する（鍵情報管理テーブルは鍵情報を複数保持しうる）。なお、一対の暗号化・復号化処理で用いられる暗号鍵と復号鍵とは、暗号化方式によって、同一である場合も異なる場合もあるが、いずれにしても同一の鍵番号によって識別される。

【００２５】

ここで、鍵情報管理テーブル２１は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持している。

【００２６】

また、コンテンツサーバ１１は、鍵管理手段１１１と、暗号化・パケット送信手段１１２とを含んで構成されている。

【００２７】

鍵管理サーバ３１は、鍵（本実施の形態では、復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル４１を有する。

【００２８】

ここで、鍵情報管理テーブル４１は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル４１は情報を持っていない。

【００２９】

また、鍵管理サーバ３１は、鍵管理手段３１１を含んで構成されている。

【００３０】

クライアント５ｉは、マルチキャストパケットによって配信されるデータの復号化に用いる鍵（復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル６ｉを有する。

【００３１】

ここで、鍵情報管理テーブル６ｉは、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル６ｉは情報を持っていない。

【００３２】

また、クライアント５ｉは、鍵管理手段５ｉ１と、パケット受信・復号化手段５ｉ２とを含んで構成されている。

【００３３】

なお、コンテンツサーバ１１，鍵管理サーバ３１，および各クライアント５ｉは、それぞれの管理する鍵情報管理テーブル２１，鍵情報管理テーブル４１，および各鍵情報管理テーブル６ｉ上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

【００３４】

図２は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。この処理は、配信データ暗号化ステップＡ１と、マルチキャストパケット送信ステップＡ２と、マルチキャストパケット受信ステップＡ３と、使用中鍵番号一致判定ステップＡ４と、次使用鍵番号一致判定ステップＡ５と、暗号化データ復号化ステップＡ６と、鍵管理サーバ問い合わせステップＡ７とからなる。

【００３５】

図３は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。この処理は、第１設定値到達認識ステップＢ１と、鍵情報メッセージ送信ステップＢ２と、鍵情報メッセージ受信ステップＢ３と、次使用鍵情報保存ステップＢ４とからなる。

【００３６】

図４は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第２設定値となった時点における処理）を示す流れ図である。この処理は、第２設定値到達認識ステップＣ１と、鍵情報要求送信ステップＣ２と、鍵情報要求受信ステップＣ３と、応答メッセージ送信ステップＣ４と、応答メッセージ受信ステップＣ５と、次使用鍵情報保存ステップＣ６とからなる。

【００３７】

図５は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【００３８】

図６は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

【００３９】

次に、図１～図６を参照して、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の全体の動作について詳細に説明する。

【００４０】

第１に、コンテンツサーバ１１から各クライアント５ｉにネットワーク１００を介して行われるマルチキャストパケット送受信処理に関する動作について説明する（図２参照）。

【００４１】

コンテンツサーバ１１内の暗号化・パケット送信手段１１２は、マルチキャスト配信時に、自身が保持している現在使用中の暗号鍵（鍵情報管理テーブル２１内の使用中の鍵に関する鍵情報中の暗号鍵）を用いて、配信データ（配信対象のデータ）の暗号化を行う（ステップＡ１）。

【００４２】

その上で、暗号化データ（暗号化された配信データ）と当該暗号鍵の鍵番号とを有するマルチキャストパケットをネットワーク１００上に送信する（ステップＡ２）。

【００４３】

マルチキャストアドレスに参加しているクライアント５ｉ内のパケット受信・復号化手段5.ｉ２は、コンテンツサーバ１１から送信されたマルチキャストパケットを受信し（ステップＡ３）、受信したマルチキャストパケットに含まれている暗号化データの復号化処理を行う。

【００４４】

この復号化処理に際しては、まず、受信したマルチキャストパケット中の鍵番号と自身が記憶している現在使用中の復号鍵の鍵番号（鍵情報管理テーブル６ｉ内の使用中の鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップＡ４）。

【００４５】

ステップＡ４で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップＡ６）。

【００４６】

一方、ステップＡ４で「両鍵番号が一致しない」と判定した場合には、当該マル

チキャストパケット中の鍵番号と自身が記憶している次に使用する復号鍵の鍵番号（鍵情報管理テーブル６ｉ内の次に使用する鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップＡ５）。

【００４７】

ステップＡ５で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップＡ６）。

【００４８】

一方、ステップＡ５で「両鍵番号が一致しない」と判定した場合（鍵情報管理テーブル６ｉ内に次に使用する鍵に関する鍵情報が存在しない場合を含む）、すなわち、使用中の鍵および次に使用する鍵のどちらの鍵番号についても当該マルチキャストパケット中の鍵番号とは一致しなかった場合には、鍵情報の取得処理が正しく行われていないことを意味するため、鍵管理サーバ３１にその旨の問い合わせを行う（ステップＡ７）。

【００４９】

第２に、使用中の鍵の残り有効時間の値が初期値（残り有効時間初期値）から第１設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【００５０】

この期間においては、コンテンツサーバ１１内の鍵情報管理テーブル２１は、使用中の鍵（暗号鍵および復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）と、次に使用する鍵（暗号鍵および復号鍵）に関する鍵情報とを保持している。これらの鍵および鍵番号は、コンテンツサーバ１１内の鍵管理手段１１１によって作成される。

【００５１】

また、この期間においては、鍵管理サーバ３１内の鍵情報管理テーブル４１は、使用中の鍵（復号鍵）に関する鍵情報を保持している。

【００５２】

さらに、この期間においては、各クライアント５ｉ内の鍵情報管理テーブル６ｉ

は、使用中の鍵（復号鍵）に関する鍵情報（コンテンツサーバ１１から使用中の鍵によって暗号化されたデータを含むマルチキャストパケットを受信するまでは、次に使用する鍵の鍵情報として管理している）を保持している。また、コンテンツサーバ１１から新たな使用中の鍵によって暗号化されたデータを有するマルチキャストパケットを受信するまでは、直前に使用中の鍵であった鍵に関する鍵情報も保持している。

【００５３】

なお、この期間に新しくマルチキャストアドレスに参加したクライアント５ｉが存在する場合に、当該クライアント５ｉ内の鍵管理手段５ｉ１が鍵管理サーバ３１に鍵情報要求８１を送信すると、鍵管理サーバ３１内の鍵管理手段３１１は使用中の鍵に関する鍵情報を有する応答メッセージ８２を当該クライアント５ｉに送信する。

【００５４】

第３に、使用中の鍵の残り有効時間の値が第１設定値となった時点における鍵管理に関する動作について説明する（図３参照）。

【００５５】

コンテンツサーバ１１内の鍵管理手段１１１は、鍵情報管理テーブル２１で管理している使用中の鍵の残り有効時間の値が第１設定値となったこと（残り有効時間の値が減っていって第１設定値に達したこと）を認識すると（ステップＢ１）、次に使用する鍵（復号鍵）に関する鍵情報（鍵番号と鍵と残り有効時間との組）を有するメッセージ（鍵情報メッセージ７１）を鍵管理サーバ３１に対して送信する（ステップＢ２）。

【００５６】

鍵管理サーバ３１内の鍵管理手段３１１は、コンテンツサーバ１１から鍵情報メッセージ７１を受信すると（ステップＢ３）、その鍵情報メッセージ７１中の次に使用する鍵に関する鍵情報を鍵情報管理テーブル４１に保存する（ステップＢ４）。これによって、鍵管理サーバ３１内の鍵情報管理テーブル４１は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【００５７】

なお、この時点から使用中の鍵の残り有効時間の値が後述の第２設定値となる時点までの期間において、新しくマルチキャストアドレスに参加したクライアント５ｉが存在する場合に、当該クライアント５ｉ内の鍵管理手段５ｉ１が鍵管理サーバ３１に鍵情報要求８１を送信すると、鍵管理サーバ３１内の鍵管理手段３１１は使用中の鍵に関する鍵情報と次に使用する鍵に関する鍵情報とを有する応答メッセージ８２を当該クライアント５ｉに送信する。

【００５８】

第４に、使用中の鍵の残り有効時間の値が第２設定値（第１設定値よりも小さい値であり０よりも大きい値）となった時点における鍵管理に関する動作について説明する（図４参照）。

【００５９】

クライアント５ｉ内の鍵管理手段５ｉ１は、自身の鍵情報管理テーブル６ｉ内の使用中の鍵の残り有効時間の値が第２設定値となった時に、そのこと（残り有効時間の値が減っていって第２設定値に達したこと）を認識し（ステップＣ１）、次に使用する鍵（復号鍵）に関する鍵情報を得るために、鍵管理サーバ３１に対して鍵情報要求８１を送信する（ステップＣ２）。なお、クライアント５ｉには、鍵情報要求８１の送信先である鍵管理サーバ３１のアドレスが、あらかじめ設定されている。

【００６０】

鍵管理サーバ３１内の鍵管理手段３１１は、クライアント５ｉからの鍵情報要求８１を受信すると（ステップＣ３）、その応答として、現在使用中の鍵（復号鍵）に関する鍵情報と次に使用する鍵（復号鍵）に関する鍵情報とを有する応答メッセージ８２を当該クライアント５ｉに送信する（ステップＣ４）。

【００６１】

当該クライアント５ｉは、この応答メッセージ８２を受信すると（ステップＣ５）、当該応答メッセージ８２中の次に使用する鍵に関する鍵情報を自己の鍵情報管理テーブル６ｉに保存する（ステップＣ６）。

【００６２】

第５に、使用中の鍵の残り有効時間の値が０となった時点における鍵管理に関する動作について説明する。

【００６３】

コンテンツサーバ１１内の鍵管理手段１１１は、鍵情報管理テーブル２１に保持されている使用中の鍵の残り有効時間が０となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル２１に保存する。これにより、暗号化・パケット送信手段１１２は、その鍵を使用して以後の暗号化処理を行う。

【００６４】

このときさらに、鍵管理手段１１１は、新たな次に使用する鍵（暗号鍵および復号鍵）を作成して、その次に使用する鍵に関する鍵情報を鍵情報管理テーブル２１に保存する。

【００６５】

また、暗号化・パケット送信手段１１２は、暗号化パケット（暗号化データを有するマルチキャストパケット）に含まれる鍵番号を新たな使用中の鍵に対する鍵番号に変更し、それにより、クライアント５ｉに対して使用中の鍵が変更されたことを示す。

【００６６】

各クライアント５ｉ内の鍵管理手段５ｉ１は、コンテンツサーバ１１から送られてきた暗号化パケット（パケット受信・復号化手段５ｉ２により受信された暗号化パケット）に含まれる鍵番号が変更されたことを確認すると、自身の鍵情報管理テーブル６ｉ内の当該鍵番号を持つ次に使用する鍵を新たな使用中の鍵として保存するようにする。このとき、当該各クライアント５ｉは、新たな次に使用する鍵をまだ得ていないため、自身の鍵情報管理テーブル６ｉにおいて次に使用する鍵に関する鍵情報を持たない状態となる。

【００６７】

一方、鍵管理サーバ３１内の鍵管理手段３１１は、鍵情報管理テーブル４１に保持されている使用中の鍵に関する鍵情報中の残り有効時間が０となった時に、そ

の使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル４１に保存する。このとき、鍵管理サーバ３１は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル４１において次に使用する鍵に関する鍵情報を持たない状態となる。

【００６８】

なお、残り有効時間の初期値，第１設定値（Ｘとする）および第２設定値（Ｙとする）の設定方法は、例えば、次のａまたはｂに示すような方法が考えられる。

【００６９】

ａ．当該マルチキャスト配信システム全体で共通な設定値として、手動での設定を行う。

【００７０】

ｂ．鍵の残り有効時間とともにその初期値を各装置（鍵管理サーバおよびクライアント）に送信することで、その初期値から一定の割合の時間をＸおよびＹとして各装置で求める。この「一定の割合」は、当該マルチキャスト配信システム全体で共通な設定とする。具体例を挙げると、Ｘを鍵の残り有効時間の初期値の５０％とし、Ｙを鍵の残り有効時間の初期値の２５％とした場合に、鍵の残り有効時間の初期値が１時間であった際には、Ｘは３０分となり、Ｙは１５分となる。

【００７１】

次に、図５および図６を参照して、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作（一連の動作シーケンス）について説明する。

【００７２】

図５は、各鍵情報管理テーブル内の情報や、各パケット／要求／メッセージの内容を具体的に示す図である。なお、図５においては、使用中の鍵を鍵Ａで示しており、次に使用する鍵を鍵Ｂで示しており、それらの鍵番号を「鍵番号Ａ」および「鍵番号Ｂ」と表記している。また、この例では、暗号鍵と復号鍵とは同じ鍵であるものとする（例えば、鍵Ａは暗号鍵でもあり、復号鍵でもある）。さらに、第１設定値をＸで示しており、第２設定値をＹで示している。

【００７３】

図６は、図５に示すような内容の情報が取り扱われる場合の動作シーケンスを時間経過に沿って示した図である。

【００７４】

この動作シーケンスでは、初期状態（鍵Ａの残り有効時間の値が初期値である状態）において、コンテンツサーバ１１は、使用中の鍵の鍵Ａと次に使用する鍵の鍵Ｂとに関する鍵情報を持っている。また、鍵管理サーバ３１およびクライアント５１（ここでは、複数のクライアント５１～５ｎの中からクライアント５１に注目する）は、図５に示す鍵情報のうちの鍵Ａに関する鍵情報のみを持っている。なお、残り有効時間の初期値や、ＸおよびＹの値は、あらかじめ、コンテンツサーバ１１，鍵管理サーバ３１，およびクライアント５１～５ｎに設定されているものとする。

【００７５】

鍵Ａの残り有効時間の値がＸ（第１設定値）となった時に、コンテンツサーバ１１は、鍵Ｂ（次に使用する鍵）に関する鍵情報を有する鍵情報メッセージ７１を鍵管理サーバ３１に対して送信する。これにより、鍵管理サーバ３１は、図５に示すように、鍵Ａと鍵Ｂとに関する鍵情報を持つことになる。

【００７６】

鍵Ａの残り有効時間の値がＹ（第２設定値）となった時に、クライアント５１は、鍵管理サーバ３１に対して、次に使用する鍵に関する鍵情報を要求する鍵情報要求８１を送信する。

【００７７】

この鍵情報要求８１を受けた鍵管理サーバ３１は、応答として、現在使用中の鍵（鍵Ａ）と次に使用する鍵（鍵Ｂ）とに関する鍵情報を有する応答メッセージ８２を送信する。これにより、クライアント５１は、図５に示すように、鍵Ａと鍵Ｂとに関する鍵情報を持つことになる。

【００７８】

鍵Ａの残り有効時間の値が０となった時に、コンテンツサーバ１１は、使用中の鍵である鍵Ａに関する鍵情報を破棄し、保存していた次に使用する鍵である鍵Ｂ

を新たな使用中の鍵として保持し、その鍵Ｂを使用して配信データの暗号化を行う。また、この時に、コンテンツサーバ１１は、新たな次に使用する鍵として鍵Ｃを生成し、この鍵Ｃに関する鍵情報を鍵情報管理テーブル２１に保存する。この鍵Ｃに関する鍵情報は、鍵Ｂの残り有効時間がＸとなった時に、鍵情報メッセージ７１によって、コンテンツサーバ１１から鍵管理サーバ３１に対して送信される。

【００７９】

鍵管理サーバ３１は、鍵Ａの残り有効時間の値が０となった時に、鍵Ａに関する鍵情報を破棄し、次に使用する鍵として保存していた鍵Ｂを現在使用中の鍵として保持する。さらに、コンテンツサーバ１１からの鍵情報メッセージ７１によって鍵Ｃに関する鍵情報を受け取ると、その鍵情報を次に使用する鍵に関する鍵情報として鍵情報管理テーブル４１に保存する。これにより、鍵情報管理テーブル４１に保持されている鍵情報は、図５中の鍵Ａに関する鍵情報が鍵Ｂに関する鍵情報に入れ替わり、図５中の鍵Ｂに関する鍵情報が鍵Ｃに関する鍵情報に入れ替わった形となる。

【００８０】

クライアント５１は、コンテンツサーバ１１から鍵Ｂの鍵番号を有するマルチキャストパケットを受信すると、鍵Ａに関する鍵情報を破棄し、次に使用する鍵として保存していた鍵Ｂを現在使用中の鍵として保持する。さらに、鍵管理サーバ３１からの応答メッセージ８２によって鍵Ｂの次に使用する鍵である鍵Ｃに関する鍵情報を受け取ると、その鍵情報を自身の鍵情報管理テーブル６ｉに保存する。これにより、当該鍵情報管理テーブル６ｉに保持されている鍵情報は、図５中の鍵Ａに関する鍵情報が鍵Ｂに関する鍵情報に入れ替わり、図５中の鍵Ｂに関する鍵情報が鍵Ｃに関する鍵情報に入れ替わった形となる。

【００８１】

以上のような動作が繰り返されることによって、クライアント５１（一般的には、各クライアント５ｉ）は鍵の変更が実行される前に、次に使用する鍵に関する鍵情報を取得することが可能になる。

【００８２】

なお、本実施の形態においては、コンテンツサーバ１１，鍵管理サーバ３１，およびクライアント５ｉの間の通信に掛かる通信遅延は考慮されていない。したがって、そのような通信遅延の分だけ、各鍵情報管理テーブル２１，４１，および６ｉにおける同一の鍵番号の鍵情報中の残り有効時間の値にずれが生じることも考えられる。このようなずれが実際に問題になる可能性は少ないが、これを考慮する際にも、以下のａおよびｂに示すように、適切な対処が可能となる。

【００８３】

ａ．使用中の鍵の有効時間が切れる前（残り有効時間が０となる前）に次に使用する予定の鍵が使用された暗号化データ（その暗号化データと次に使用する鍵の鍵番号とを有するマルチキャストパケット）がきても、クライアント５ｉは、上記のような構成・動作によって、次に使用する鍵に関する鍵情報を保持しているため、鍵（復号鍵）の特定が可能であり、その復号鍵による解読（復号化）が可能となる。

【００８４】

ｂ．有効時間が切れた後に古い鍵を使用した暗号化データが送られてきたとしても、クライアント５ｉは、残り有効時間が０となった後も、新たな使用中の鍵の鍵番号を有するマルチキャストパケットを受信するまでは、古い鍵に関する鍵情報を保持しているので、その鍵（復号鍵）による解読が可能となる。

【００８５】

（２）　第１の実施の形態の変形形態

【００８６】

上記のような第１の実施の形態に対しては、コンテンツサーバ１１からクライアント５ｉに配信されるマルチキャストパケットに含まれる情報に関して、以下のａおよびｂに示すような変形形態を考えることができる（ａおよびｂを併有する形態も可能である）。

【００８７】

ａ．上記の第１の実施の形態では、マルチキャストパケットは暗号化データと鍵番号とを有していたが、これに対して、さらに、鍵管理サーバ３１のアドレス（アドレスと同様に問合せ先を示す情報を含む）を付加することも可能である。こ

のように、マルチキャストパケット中に鍵管理サーバアドレスを付加して送ることによって、クライアント５ｉ側で鍵情報の問合せ・要求先（鍵情報要求８１の送信先）の設定を不要にすることができる。

【００８８】

ｂ．また、マルチキャストパケットには、そのマルチキャストパケットが有している鍵番号で識別される鍵の残り有効時間を付加することも可能である。

【００８９】

（３）　第２の実施の形態

【００９０】

図７は、本発明の第２の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【００９１】

図７を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ１２と、コンテンツサーバ１２より送られたマルチキャストパケットを受信するクライアント５１，５２，…，５ｎ（ｎは正整数）と、コンテンツサーバ１２から送られた鍵作成要求９１に応じて鍵（暗号鍵および復号鍵）を作成・保管して当該暗号鍵とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を有する鍵情報応答メッセージ９２をコンテンツサーバ１２に返送し、クライアント５ｉ（ｉは１～ｎの正整数）からの鍵情報要求８１に対して応答メッセージ８２を送信する鍵管理サーバ３２と、コンテンツサーバ１２，クライアント５ｉ，および鍵管理サーバ３２を接続するネットワーク１００とを含んで構成されている。

【００９２】

コンテンツサーバ１２は、マルチキャストパケットによって配信されるデータの暗号化に用いる鍵（暗号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル２２を有する（鍵情報管理テーブルは鍵情報を複数保持しうる）。

【００９３】

ここで、鍵情報管理テーブル２２は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。

【００９４】

また、コンテンツサーバ１２は、鍵管理手段１２１と、暗号化・パケット送信手段１２２とを含んで構成されている。

【００９５】

鍵管理サーバ３２は、鍵（暗号鍵・復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル４２を有する。なお、本実施の形態では、鍵管理サーバ３２によって鍵の作成が行われるので、鍵管理サーバ３２の鍵情報管理テーブル４２が暗号鍵と復号鍵とに関する鍵情報を保持している。

【００９６】

ここで、鍵情報管理テーブル４２は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持している。

【００９７】

また、鍵管理サーバ３２は、鍵管理手段３２１を含んで構成されている。

【００９８】

クライアント５ｉは、マルチキャストパケットによって配信されるデータの復号化に用いる鍵（復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル６ｉを有する。

【００９９】

ここで、鍵情報管理テーブル６ｉは、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル６ｉは情報を持っていない。

【０１００】

また、クライアント５ｉは、鍵管理手段５ｉ１と、パケット受信・復号化手段５ｉ２とを含んで構成されている。

【０１０１】

なお、コンテンツサーバ１２，鍵管理サーバ３２，および各クライアント５ｉは

、それぞれの管理する鍵情報管理テーブル２２，鍵情報管理テーブル４２，および各鍵情報管理テーブル６ｉ上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

【０１０２】

本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、第１の実施の形態と比較して、コンテンツサーバ１２が鍵管理サーバ３２に対して鍵作成要求９１を送信し、それに応じて、鍵管理サーバ３２が鍵（暗号鍵・復号鍵）を作成し、作成した暗号鍵に関する鍵情報を有する鍵情報応答メッセージ９２をコンテンツサーバ１２に対して返送する点が異なっている。

【０１０３】

図８は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。この処理は、第１設定値到達認識ステップＤ１と、鍵作成要求送信ステップＤ２と、鍵作成要求受信ステップＤ３と、次使用鍵作成ステップＤ４と、次使用鍵情報保存ステップＤ５と、鍵情報応答メッセージ送信ステップＤ６と、鍵情報応答メッセージ受信ステップＤ７と、次使用鍵情報保存ステップＤ８とからなる。

【０１０４】

次に、図７および図８を参照して（図１～図４も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の動作について、第１の実施の形態とは異なる点を中心にして説明する。

【０１０５】

第１に、コンテンツサーバ１２から各クライアント５ｉにネットワーク１００を介して行われるマルチキャストパケット送受信処理に関する動作について説明する。

【０１０６】

この動作は、第１の実施の形態における動作（図１中のコンテンツサーバ１１から各クライアント５ｉにネットワーク１００を介して行われるマルチキャストパケット送受信処理に関する動作）と同様なものとなる。

【０１０７】

第２に、使用中の鍵の残り有効時間の値が初期値から第１設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【０１０８】

この期間においては、コンテンツサーバ１２内の鍵情報管理テーブル２２は、使用中の鍵（暗号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ３２内の鍵管理手段３２１によって作成されたものである。

【０１０９】

また、この期間においては、鍵管理サーバ３２内の鍵情報管理テーブル４２は、使用中の鍵（暗号鍵・復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ３２内の鍵管理手段３２１によって作成されたものである。

【０１１０】

なお、上記以外の動作は、第１の実施の形態における動作と同様なものとなる。

【０１１１】

第３に、使用中の鍵の残り有効時間の値が第１設定値となった時点における鍵管理に関する動作について説明する（図８参照）。

【０１１２】

第１の実施の形態では、コンテンツサーバ１１は、使用中の鍵の残り有効時間の値が第１設定値となったことを認識すると、鍵情報メッセージ７１を鍵管理サーバ３１に送信していた。

【０１１３】

これに対して、本実施の形態では、コンテンツサーバ１２内の鍵管理手段１２１は、鍵情報管理テーブル２２で管理している使用中の鍵の残り有効時間の値が第１設定値となったこと（その時点に達したこと）を認識すると（ステップＤ１）、次に使用する鍵（暗号鍵）の鍵情報を得るために、鍵作成要求９１を鍵管理サーバ３２に対して送信する（ステップＤ２）。

【０１１４】

鍵管理サーバ３２内の鍵管理手段３２１は、コンテンツサーバ１２から鍵作成要求９１を受信すると（ステップＤ３）、その鍵作成要求９１に応じて、次に使用する鍵（暗号鍵・復号鍵）を作成し（ステップＤ４）、その鍵に関する鍵情報（鍵と鍵番号と残り有効時間との組）を鍵情報管理テーブル４２に保存する（ステップＤ５）。これによって、鍵管理サーバ３２内の鍵情報管理テーブル４２は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【０１１５】

さらに、鍵管理手段３２１は、ステップＤ４で作成した暗号鍵に関する鍵情報（暗号鍵と鍵番号と残り有効時間との組）を有する鍵情報応答メッセージ９２をコンテンツサーバ１２に送信（返送）する（ステップＤ６）。

【０１１６】

コンテンツサーバ１２内の鍵管理手段１２１は、鍵管理サーバ３２から鍵情報応答メッセージ９２を受信すると（ステップＤ７）、その鍵情報応答メッセージ９２中の次に使用する鍵（暗号鍵）に関する鍵情報を鍵情報管理テーブル２２に保存する（ステップＤ８）。これによって、コンテンツサーバ１２内の鍵情報管理テーブル２２は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【０１１７】

なお、上記以外の動作は、第１の実施の形態における動作と同様なものとなる。

【０１１８】

第４に、使用中の鍵の残り有効時間の値が第２設定値（第１設定値よりも小さい値であり０よりも大きい値）となった時点における鍵管理に関する動作について説明する。

【０１１９】

この動作は、第１の実施の形態における動作と同様なものとなる。

【０１２０】

第５に、使用中の鍵の残り有効時間の値が０となった時点における鍵管理に関する動作について説明する。

【０１２１】

コンテンツサーバ１２内の鍵管理手段１２１は、鍵情報管理テーブル２２に保持されている使用中の鍵の残り有効時間が０となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル２２に保存する。このとき、コンテンツサーバ１２は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル２２において次に使用する鍵に関する鍵情報を持たない状態となる。

【０１２２】

これにより、暗号化・パケット送信手段１２２は、その鍵（暗号鍵）を使用して以後の暗号化処理を行う。

【０１２３】

なお、上記以外の動作は、第１の実施の形態における動作と同様なものとなる。

【０１２４】

前述の第１の実施の形態では、コンテンツサーバ１１と鍵管理サーバ３１との間の通信に障害が発生した際に、鍵（復号鍵）の配布ができなくなることがあった。これに対して、本実施の形態（第２の実施の形態）では、コンテンツサーバ１２と鍵管理サーバ３２との間の通信に障害が発生した際にも、以前の鍵を使い続けることで、暗号化データを有するマルチキャストパケットの通信を続けることが可能になる。

【０１２５】

このように、本発明では、上記の第１の実施の形態と第２の実施の形態とに示すように、鍵をコンテンツサーバで作成する構成も、鍵管理サーバで作成する構成も、実現することが可能である。

【０１２６】

（４）　第２の実施の形態の変形形態

【０１２７】

上記の第２の実施の形態に対しても、（２）のａおよびｂで述べた第１の実施の形態に対する変形形態と同様の変形形態を考えることができる。

【０１２８】

（５）　第３の実施の形態

【０１２９】

図９は、本発明の第３の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【０１３０】

図９を参照すると、本発明の第３の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図１に示した第１の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム９０１，鍵管理サーバ用鍵交換制御プログラム９０２，およびクライアント用鍵交換制御プログラム９０３を備える点が異なっている。

【０１３１】

コンテンツサーバ用鍵交換制御プログラム９０１は、コンテンツサーバ１１に読み込まれ、当該コンテンツサーバ１１の動作を鍵情報管理テーブル２１，鍵管理手段１１１，および暗号化・パケット送信手段１１２として制御する。コンテンツサーバ用鍵交換制御プログラム９０１の制御によるコンテンツサーバ１１の動作（鍵情報管理テーブル２１，鍵管理手段１１１，および暗号化・パケット送信手段１１２に関する動作）は、第１の実施の形態におけるコンテンツサーバ１１の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３２】

また、鍵管理サーバ用鍵交換制御プログラム９０２は、鍵管理サーバ３１に読み込まれ、当該鍵管理サーバ３１の動作を鍵情報管理テーブル４１および鍵管理手段３１１として制御する。鍵管理サーバ用鍵交換制御プログラム９０２の制御による鍵管理サーバ３１の動作（鍵情報管理テーブル４１および鍵管理手段３１１に関する動作）は、第１の実施の形態における鍵管理サーバ３１の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３３】

さらに、クライアント用鍵交換制御プログラム９０３は、各クライアント５ｉに読み込まれ、当該各クライアント５ｉの動作を鍵情報管理テーブル６ｉ，鍵管理

手段５ｉｌ，およびパケット受信・復号化手段５ｉ２として制御する。クライアント用鍵交換制御プログラム９０３の制御による各クライアント５ｉの動作（鍵情報管理テーブル６ｉ，鍵管理手段５ｉ１，およびパケット受信・復号化手段５ｉ２に関する動作）は、第１の実施の形態におけるクライアント５ｉの動作と全く同様になるので、その詳しい説明を割愛する。

【０１３４】

（６）　第４の実施の形態

【０１３５】

図１０は、本発明の第４の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【０１３６】

図１０を参照すると、本発明の第４の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図７に示した第２の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム１００１，鍵管理サーバ用鍵交換制御プログラム１００２，およびクライアント用鍵交換制御プログラム１００３を備える点が異なっている。

【０１３７】

コンテンツサーバ用鍵交換制御プログラム１００１は、コンテンツサーバ１２に読み込まれ、当該コンテンツサーバ１２の動作を鍵情報管理テーブル２２，鍵管理手段１２１，および暗号化・パケット送信手段１２２として制御する。コンテンツサーバ用鍵交換制御プログラム１００１の制御によるコンテンツサーバ１２の動作（鍵情報管理テーブル２２，鍵管理手段１２１，および暗号化・パケット送信手段１２２に関する動作）は、第２の実施の形態におけるコンテンツサーバ１２の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３８】

また、鍵管理サーバ用鍵交換制御プログラム１００２は、鍵管理サーバ３２に読み込まれ、当該鍵管理サーバ３２の動作を鍵情報管理テーブル４２および鍵管理手段３２１として制御する。鍵管理サーバ用鍵交換制御プログラム１００２の制御による鍵管理サーバ３２の動作（鍵情報管理テーブル４２および鍵管理手段３

２１に関する動作）は、第２の実施の形態における鍵管理サーバ３２の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３９】

さらに、クライアント用鍵交換制御プログラム１００３は、各クライアント５ｉに読み込まれ、当該各クライアント５ｉの動作を鍵情報管理テーブル６ｉ，鍵管理手段５ｉ１，およびパケット受信・復号化手段５ｉ２として制御する。クライアント用鍵交換制御プログラム１００３の制御による各クライアント５ｉの動作（鍵情報管理テーブル６ｉ，鍵管理手段５ｉ１，およびパケット受信・復号化手段５ｉ２に関する動作）は、第２の実施の形態におけるクライアント５ｉの動作と全く同様になるので、その詳しい説明を割愛する。

【０１４０】

【発明の効果】

以上説明したように、本発明によると、以下に示すような効果が生じる。

【０１４１】

第１の効果は、鍵の変更時に新しい鍵の取得のための遅延が発生しないことにある。すなわち、鍵交換遅延のないマルチキャスト配信時の鍵の変更が可能になるということである。このような効果が生じる理由は、鍵自体とともに鍵番号および鍵の残り有効時間を有する鍵情報を管理し、クライアントが使用中の鍵の有効期間内に次に使用する鍵をあらかじめ取得することができるようにすることにより、鍵を交換した際に即時に新しい鍵を用いて復号化を行うことができるためである。

【０１４２】

第２の効果は、クライアントがどのマルチキャストアドレスに参加する際でも鍵を要求する鍵管理サーバのアドレスを当該クライアントに設定する必要がなくなることにある。このような効果が生じる理由は、コンテンツサーバが送信するマルチキャストパケットに鍵管理サーバのアドレスを含めることができるため、クライアントはその鍵管理サーバアドレスに対して鍵の要求を行うことができるからである。

【０１４３】

第３の効果は、視聴者（クライアント）の情報を正確にリアルタイムに取得できることにある。このような効果が生じる理由は、本発明を用いることで鍵変更時の遅延がなくなるため、通信遅延を増大させずに鍵の変更サイクルを短くすることができ、クライアントの情報を鍵管理サーバで集計するサイクル（クライアントが復号化のために所定時間毎に鍵管理サーバに対して行う鍵取得の要求の際に当該クライアントの情報を鍵管理サーバで集計するサイクル）も短くでき、より正確なクライアントの情報を取得することができるからである。

【０１４４】

第４の効果は、「暗号化によって視聴者（クライアント）を限定し、許可しない相手が情報を取得することを防ぐ」という暗号化方式による利点を、より確実に実現することができることにある。このような効果が生じる理由は、上記のように本発明では鍵を一定時間毎に変更することを効率的に実現できるため、万一鍵が漏れたとしても、鍵の変更により不正者が連続して視聴することを防ぐことができるからである。また、復号化に必要な鍵を管理する鍵管理サーバに視聴を許可する相手または許可しない相手を設定することで、復号鍵を渡す相手を特定することができるからでもある。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図２】

図１に示すマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。

【図３】

図１に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。

【図４】

図１に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処

理（使用中の鍵の残り有効時間の値が第２設定値となった時点における処理）を示す流れ図である。

【図５】

図１に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【図６】

図１に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

【図７】

本発明の第２の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図８】

図７に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。

【図９】

本発明の第３の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図１０】

本発明の第４の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【符号の説明】

１１，１２　コンテンツサーバ

２１，２２，４１，４２，６１，６２，…，６ｎ　鍵情報管理テーブル

３１，３２　鍵管理サーバ

５１，５２，…，５ｎ　クライアント

７１　鍵情報メッセージ

８１　鍵情報要求

８２　応答メッセージ

９１　鍵作成要求

９２　鍵情報応答メッセージ

１００　ネットワーク

１１１，１２１，３１１，３２１，５１１，５２１，…，５ｎ１　鍵管理手段

１１２，１２２　暗号化・パケット送信手段

５１２，５２２，…，５ｎ２　パケット受信・復号化手段

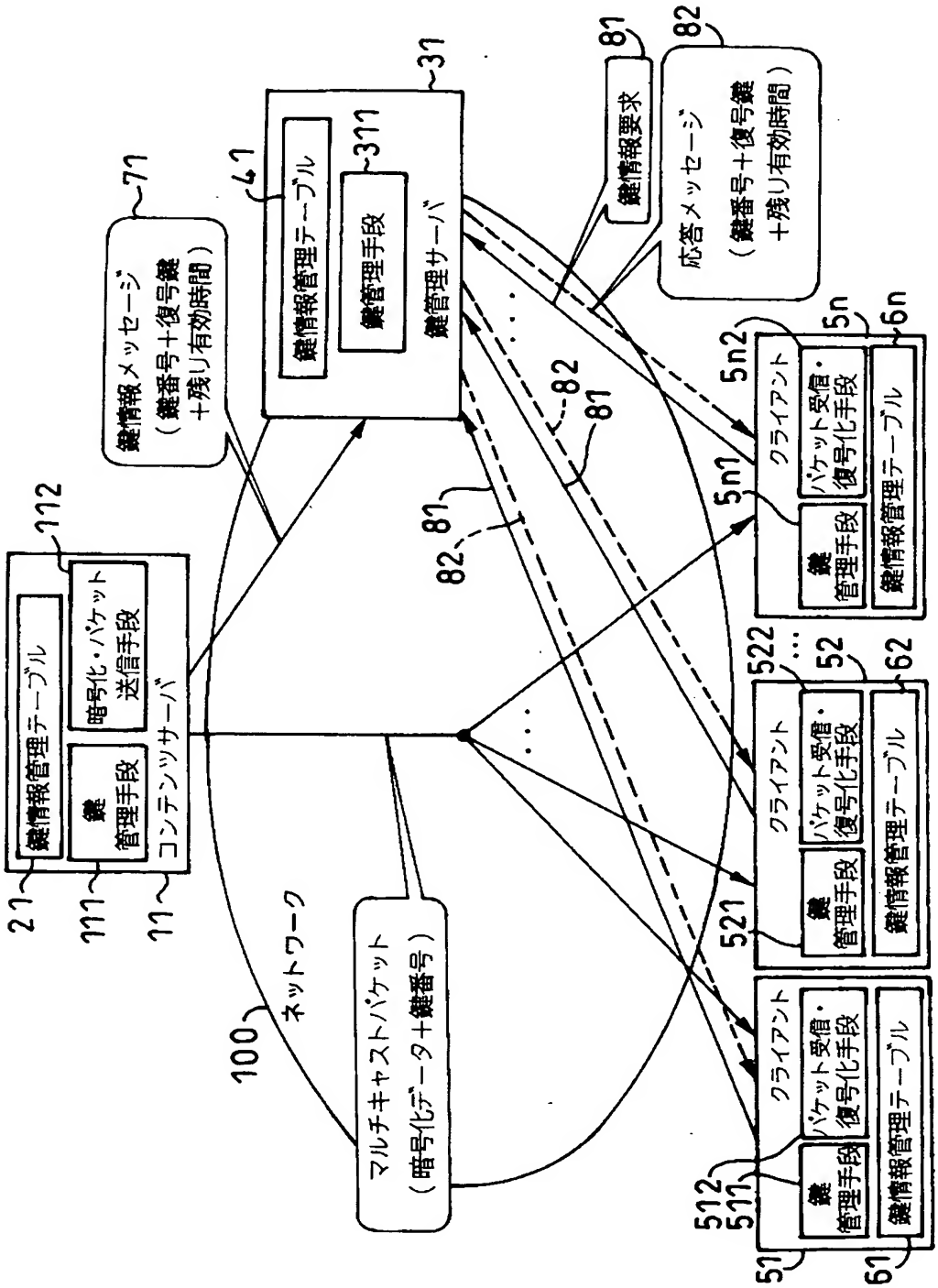
９０１，１００１　コンテンツサーバ用鍵交換制御プログラム

９０２，１００２　鍵管理サーバ用鍵交換制御プログラム

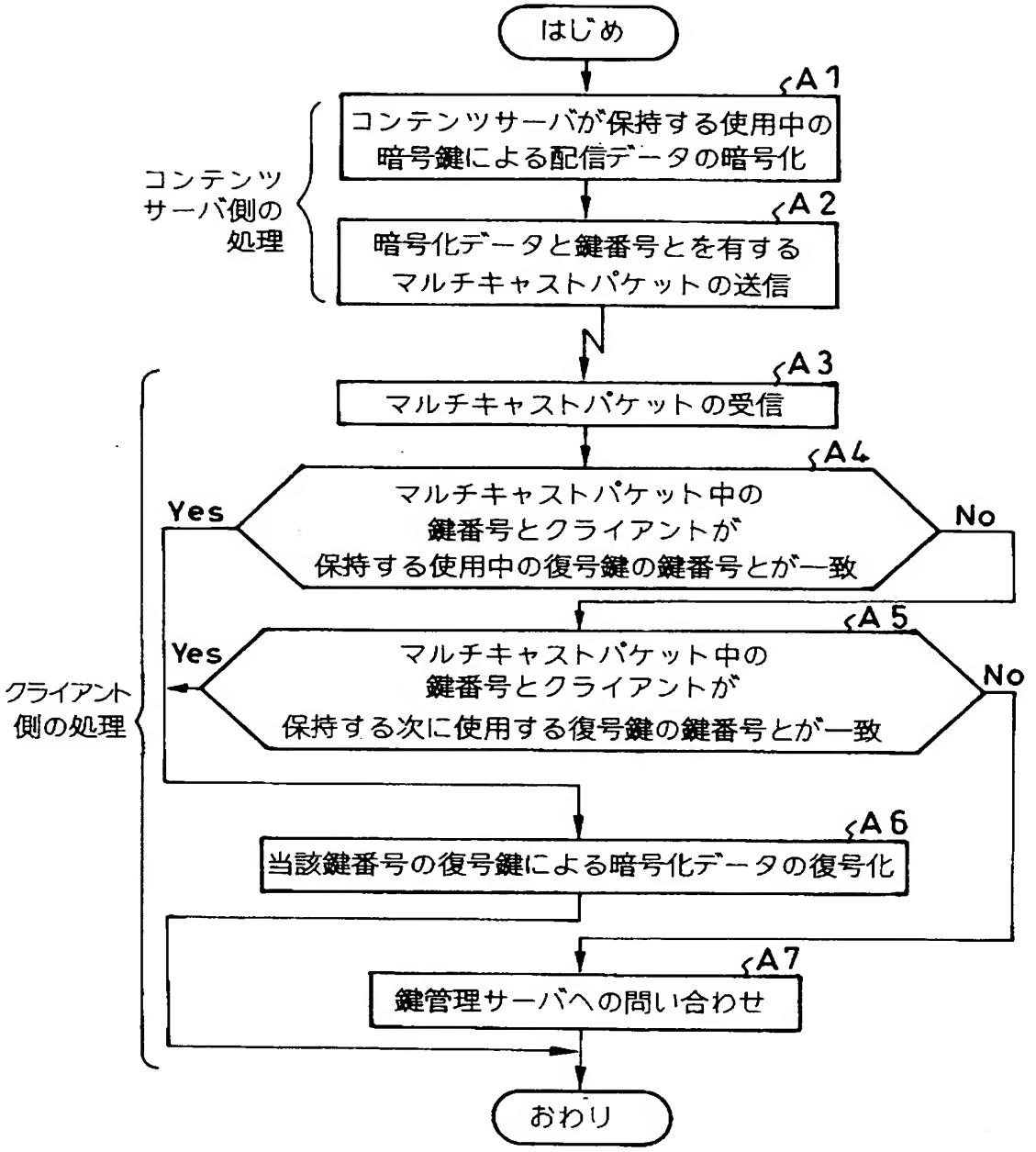
９０３，１００３　クライアント用鍵交換制御プログラム

【書類名】　図面

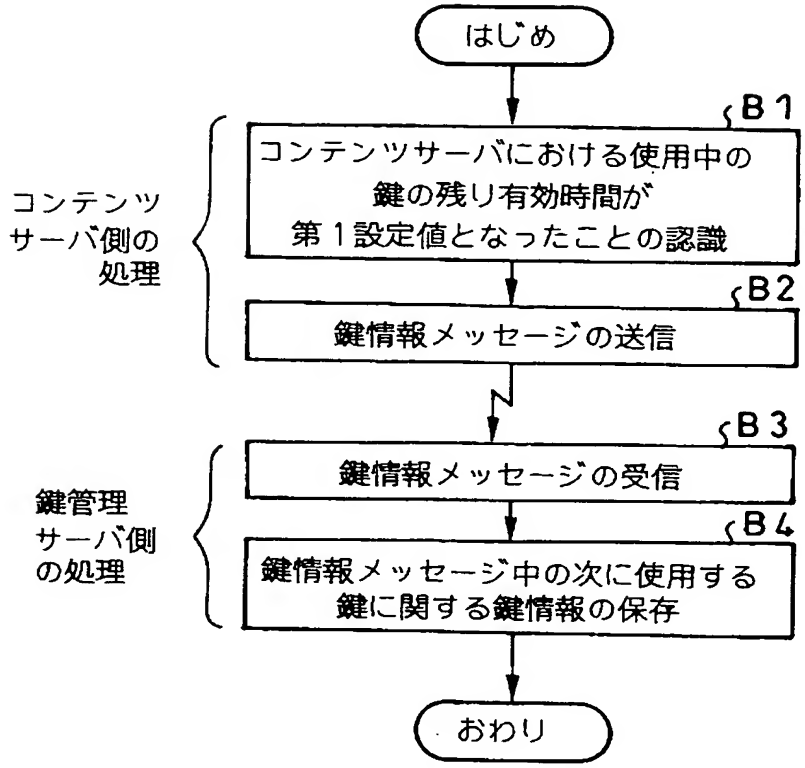
【図１】


鍵情報管理テーブル
鍵管理手段
暗号化・パケット送信手段
コンテンツサーバ
鍵情報メッセージ（鍵番号＋復号鍵＋残り有効時間）
鍵情報管理テーブル
鍵管理手段
鍵管理サーバ
鍵情報要求
応答メッセージ（鍵番号＋復号鍵＋残り有効時間）
ネットワーク
マルチキャスト/パケット（暗号化データ＋鍵番号）
クライアント
鍵管理手段
パケット受信・復号化手段
鍵情報管理テーブル
21
111
112
11
100
71
41
311
31
81
82
5n1
5n2
5n
6n
521
522
52
62
511
512
51
61

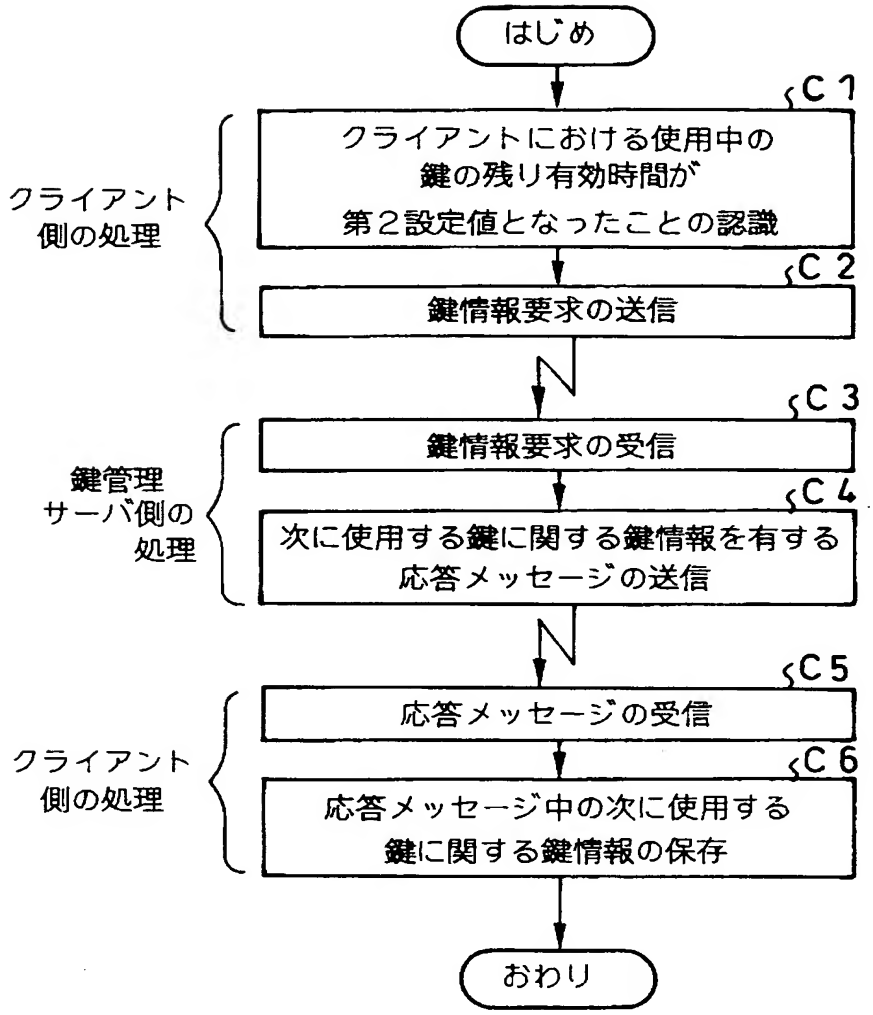
【図２】


はじめ
A1
コンテンツサーバが保持する使用中の暗号鍵による配信データの暗号化
コンテンツサーバ側の処理
A2
暗号化データと鍵番号とを有するマルチキャストパケットの送信
A3
マルチキャストパケットの受信
A4
マルチキャストパケット中の鍵番号とクライアントが保持する使用中の復号鍵の鍵番号とが一致
Yes
No
A5
マルチキャストパケット中の鍵番号とクライアントが保持する次に使用する復号鍵の鍵番号とが一致
Yes
No
クライアント側の処理
A6
当該鍵番号の復号鍵による暗号化データの復号化
A7
鍵管理サーバへの問い合わせ
おわり

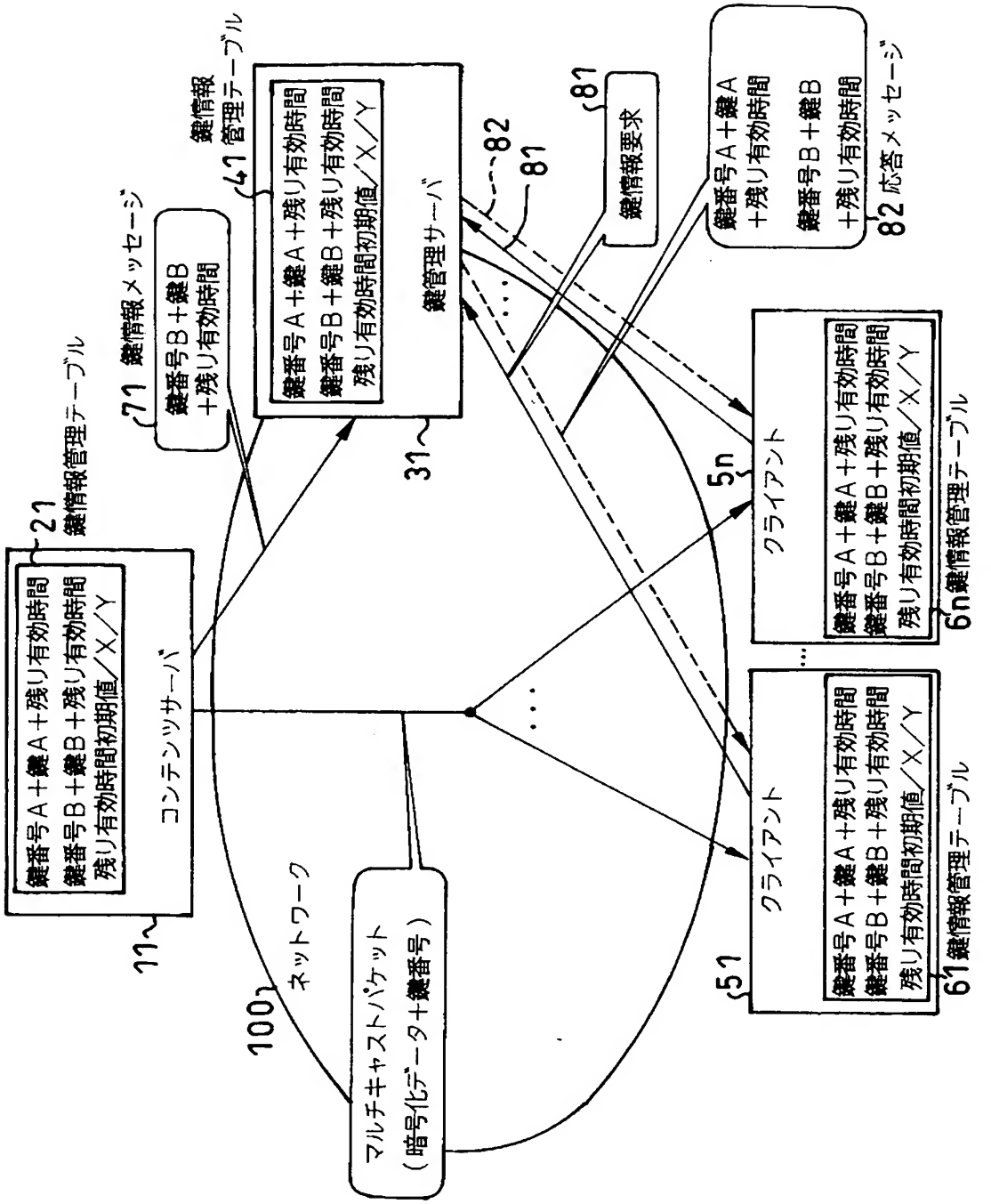
【図３】


はじめ
B1
コンテンツサーバにおける使用中の鍵の残り有効時間が第１設定値となったことの認識
B2
鍵情報メッセージの送信
B3
鍵情報メッセージの受信
B4
鍵情報メッセージ中の次に使用する鍵に関する鍵情報の保存
おわり
コンテンツサーバ側の処理
鍵管理サーバ側の処理

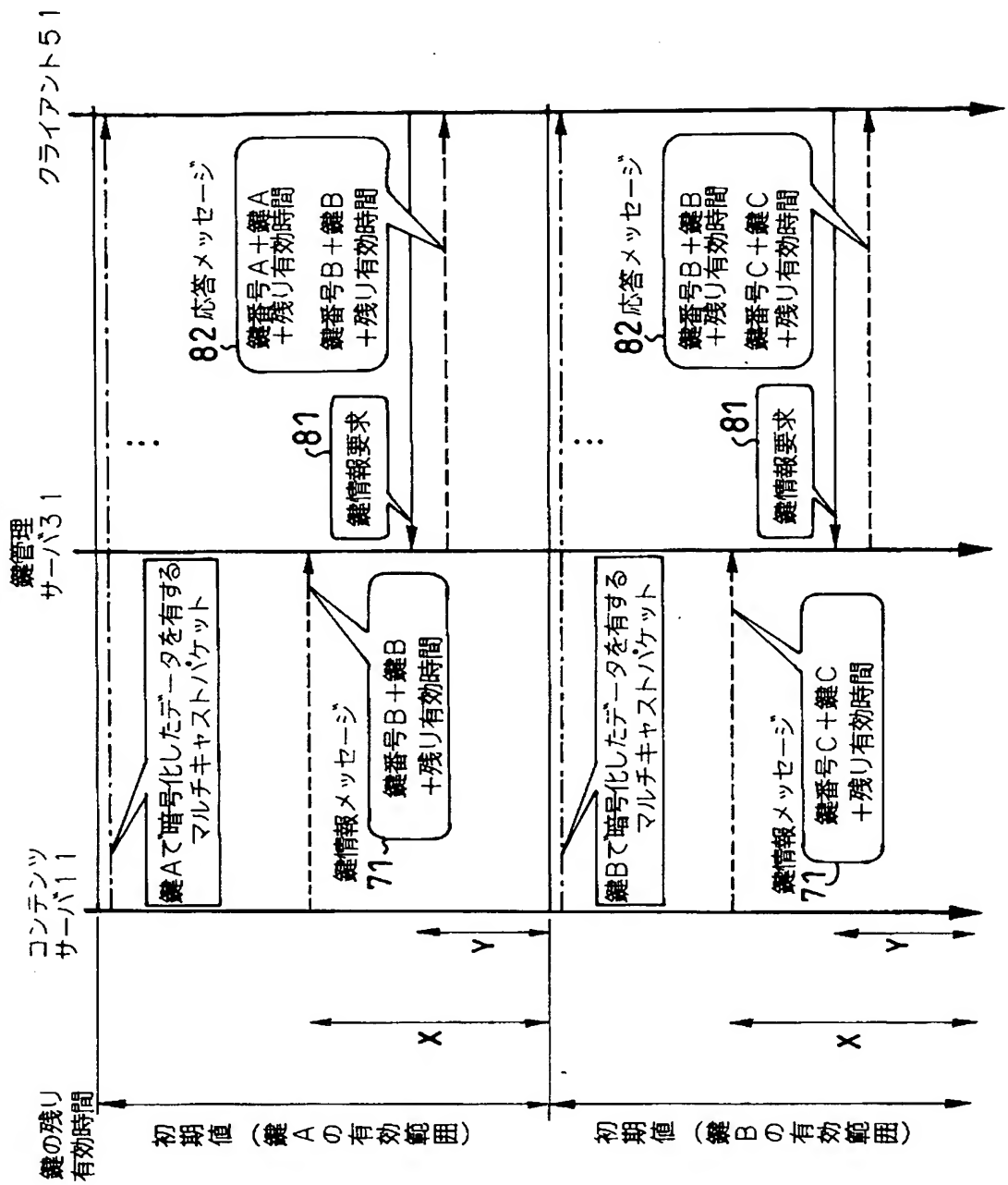
【図４】


はじめ
C 1
クライアントにおける使用中の
鍵の残り有効時間が
第２設定値となったことの認識
C 2
鍵情報要求の送信
クライアント
側の処理
C 3
鍵情報要求の受信
C 4
次に使用する鍵に関する鍵情報を有する
応答メッセージの送信
鍵管理
サーバ側の
処理
C 5
応答メッセージの受信
C 6
応答メッセージ中の次に使用する
鍵に関する鍵情報の保存
クライアント
側の処理
おわり

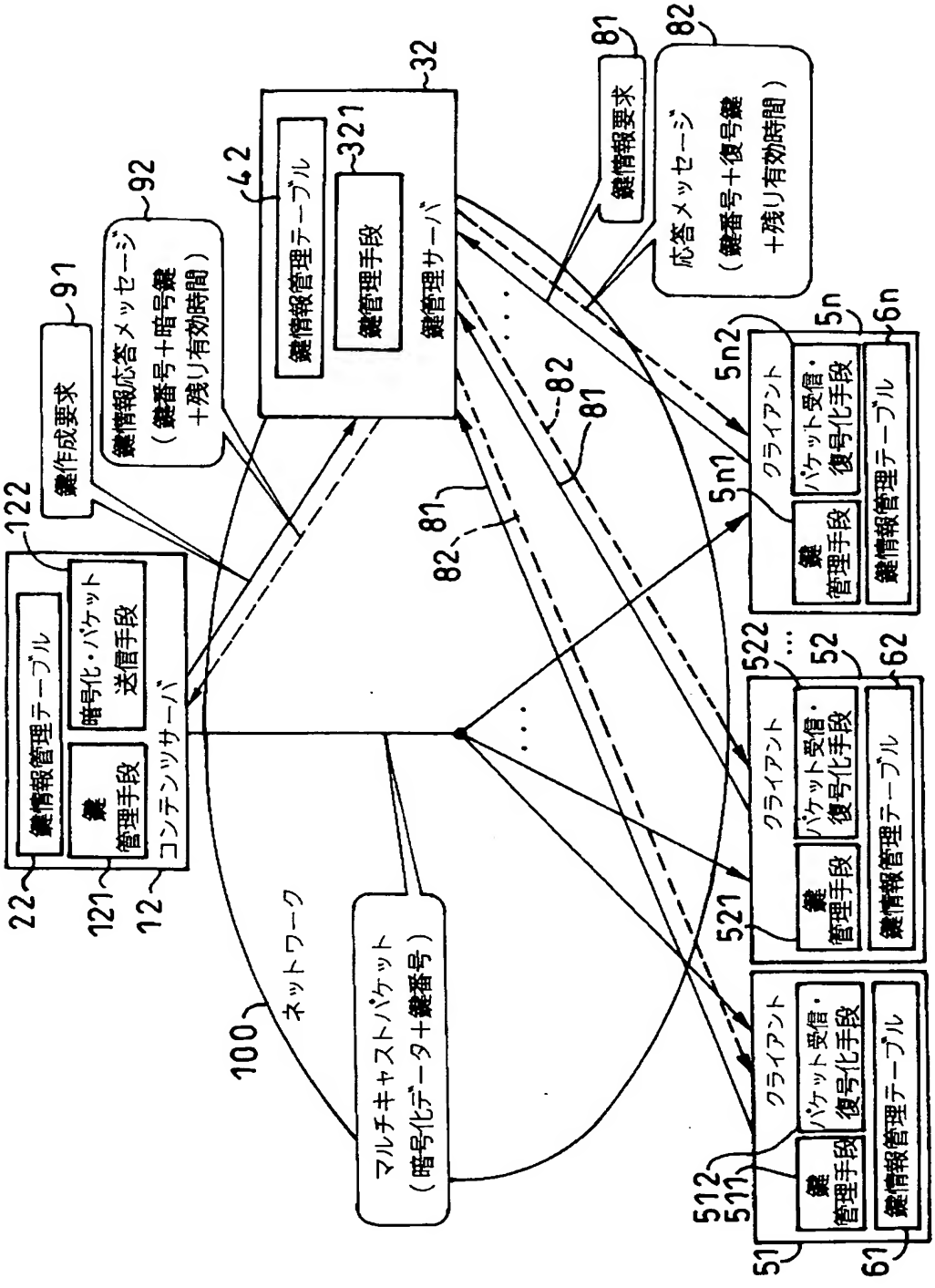
【図５】


鍵番号Ａ＋鍵Ａ＋残り有効時間
鍵番号Ｂ＋鍵Ｂ＋残り有効時間
残り有効時間初期値／Ｘ／Ｙ
コンテンツサーバ
21 鍵情報管理テーブル
11
鍵番号Ｂ＋鍵Ｂ
＋残り有効時間
71 鍵情報メッセージ
鍵情報
管理テーブル
41
鍵番号Ａ＋鍵Ａ＋残り有効時間
鍵番号Ｂ＋鍵Ｂ＋残り有効時間
残り有効時間初期値／Ｘ／Ｙ
鍵管理サーバ
31
82
81
81
鍵情報要求
鍵番号Ａ＋鍵Ａ
＋残り有効時間
鍵番号Ｂ＋鍵Ｂ
＋残り有効時間
82 応答メッセージ
5n
クライアント
鍵番号Ａ＋鍵Ａ＋残り有効時間
鍵番号Ｂ＋鍵Ｂ＋残り有効時間
残り有効時間初期値／Ｘ／Ｙ
6n 鍵情報管理テーブル
51
クライアント
鍵番号Ａ＋鍵Ａ＋残り有効時間
鍵番号Ｂ＋鍵Ｂ＋残り有効時間
残り有効時間初期値／Ｘ／Ｙ
61 鍵情報管理テーブル
100
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵番号）

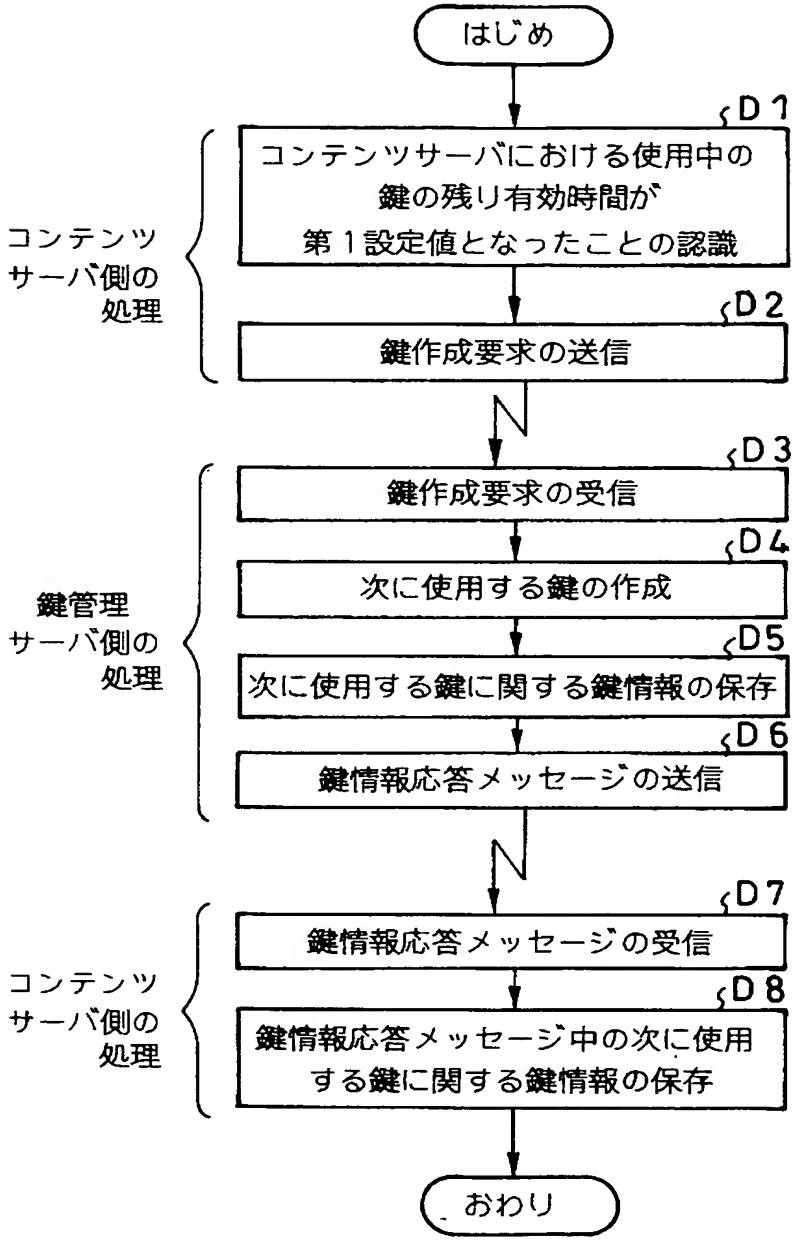
【図６】


クライアント51
鍵管理サーバ31
コンテンツサーバ11
82 応答メッセージ
鍵番号A＋鍵A＋残り有効時間
鍵番号B＋鍵B＋残り有効時間
81 鍵情報要求
鍵Aで暗号化したデータを有するマルチキャストパケット
鍵情報メッセージ 71
鍵番号B＋鍵B＋残り有効時間
鍵Bで暗号化したデータを有するマルチキャストパケット
鍵番号B＋鍵B＋残り有効時間
鍵番号C＋鍵C＋残り有効時間
鍵の残り有効時間
初期値（鍵Aの有効範囲）
初期値（鍵Bの有効範囲）
X
Y

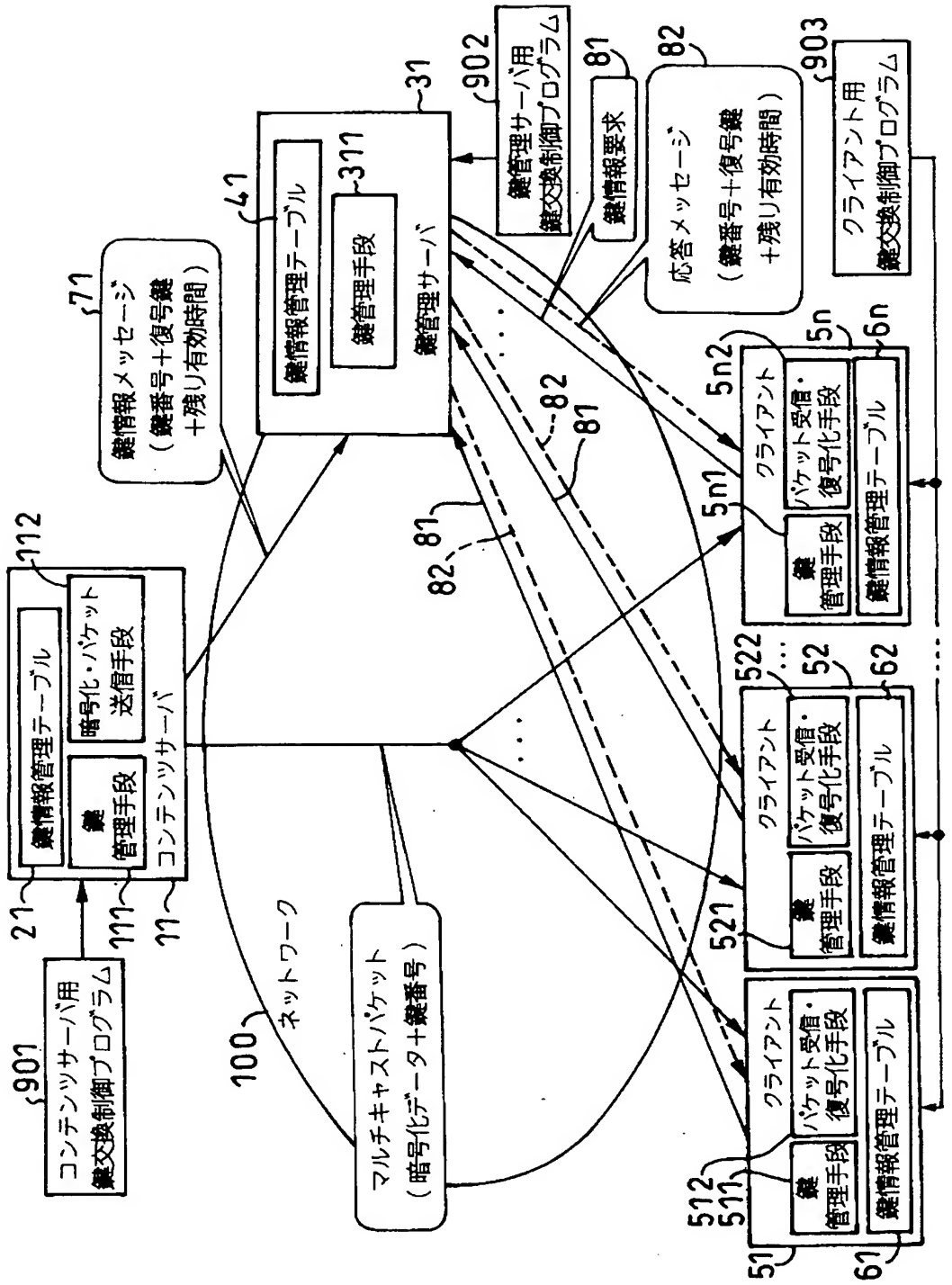
【図７】


鍵情報管理テーブル
鍵管理手段
暗号化・パケット送信手段
コンテンツサーバ
22
121
12
122
鍵作成要求
91
鍵情報応答メッセージ
（鍵番号＋暗号鍵＋残り有効時間）
92
鍵情報管理テーブル
鍵管理手段
鍵管理サーバ
42
321
32
鍵情報要求
81
応答メッセージ
（鍵番号＋復号鍵＋残り有効時間）
82
ネットワーク
100
マルチキャストパケット
（暗号化データ＋鍵番号）
クライアント
鍵管理手段
パケット受信・復号化手段
鍵情報管理テーブル
51
512
511
61
52
522
62
521
5n1
5n2
5n
6n

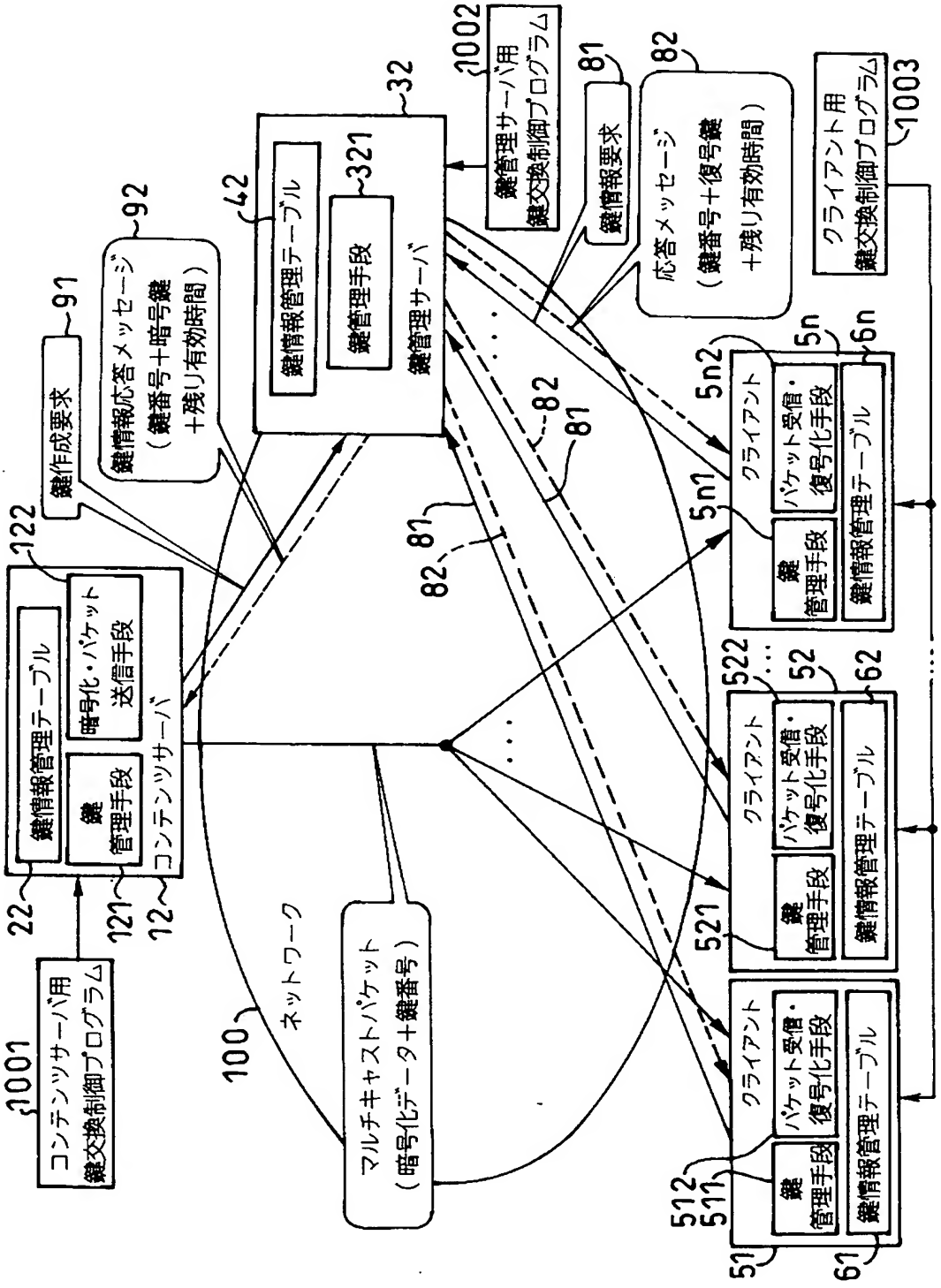
【図８】


はじめ
D1
コンテンツサーバにおける使用中の鍵の残り有効時間が第１設定値となったことの認識
D2
鍵作成要求の送信
コンテンツサーバ側の処理
D3
鍵作成要求の受信
D4
次に使用する鍵の作成
D5
次に使用する鍵に関する鍵情報の保存
D6
鍵情報応答メッセージの送信
鍵管理サーバ側の処理
D7
鍵情報応答メッセージの受信
D8
鍵情報応答メッセージ中の次に使用する鍵に関する鍵情報の保存
コンテンツサーバ側の処理
おわり

【図９】


鍵情報メッセージ
（鍵番号＋復号鍵
＋残り有効時間）
71
鍵情報管理テーブル
41
鍵管理手段
311
鍵管理サーバ
31
902
鍵管理サーバ用
鍵交換制御プログラム
81
鍵情報要求
82
応答メッセージ
（鍵番号＋復号鍵
＋残り有効時間）
903
クライアント用
鍵交換制御プログラム
鍵情報管理テーブル
112
鍵
管理手段
暗号化・パケット
送信手段
コンテンツサーバ
21
111
11
901
コンテンツサーバ用
鍵交換制御プログラム
100
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵番号）
5n2
5n1
5n
6n
クライアント
パケット受信・
復号化手段
鍵
管理手段
鍵情報管理テーブル
522
52
62
521
512
511
51
61

【図１０】


1001
コンテンツサーバ用
鍵交換制御プログラム
22
121
12
122
鍵情報管理テーブル
鍵
管理手段
暗号化・パケット
送信手段
コンテンツサーバ
91
鍵作成要求
92
鍵情報応答メッセージ
（鍵番号＋暗号鍵
＋残り有効時間）
42
鍵情報管理テーブル
321
鍵管理手段
32
鍵管理サーバ
1002
鍵管理サーバ用
鍵交換制御プログラム
81
鍵情報要求
82
応答メッセージ
（鍵番号＋復号鍵
＋残り有効時間）
1003
クライアント用
鍵交換制御プログラム
100
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵番号）
5n
6n
5n2
5n1
クライアント
パケット受信・
復号化手段
鍵
管理手段
鍵情報管理テーブル
522
52
62
521
512
511
51
61

【書類名】　要約書

【要約】

【課題】　鍵変更（交換）時に、新しい復号鍵をクライアントが取得するために生じる処理の遅延を回避する。

【解決手段】　コンテンツサーバ１１は、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバ３１に配布し、鍵番号を含むマルチキャストパケットを送信する。各クライアント５１～５ｎは、使用中の鍵の有効時間内であってコンテンツサーバ１１が鍵管理サーバ３１に次に使用する復号鍵を配布した後の時点に、鍵管理サーバ３１に対して当該次に使用する復号鍵の送付を要求する。また、マルチキャストパケット中の鍵番号に対応する復号鍵により当該マルチキャストパケット中の暗号化データの復号化を行う。鍵管理サーバ３１は、コンテンツサーバ１１から次に使用する復号鍵を受け取り、各クライアント５１～５ｎからの送付要求に応じて当該次に使用する復号鍵をその要求元に送信する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－３３２４０４
受付番号	５０２０１７３１５２６
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年１１月１８日

＜認定情報・付加情報＞

【提出日】　平成14年11月15日

次頁無

特願２００２－３３２４０４

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社

特願２００２－３３２４０４

出　願　人　履　歴　情　報

識別番号　　［０００２３２２５４］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都港区三田１丁目４番２８号
氏　名　　日本電気通信システム株式会社